GSA Students' Association

# GSASA Data Protection Policy

# 1. Introduction

This Data Protection Policy describes how personal data must be collected, handled and stored to meet the Glasgow School of Art Student Association's data protection standards and to comply with the General Data Protection Regulation (EU) 2016/679 (GDPR) and Data Protection Act 2018.

The Glasgow School of Art Students' Association (GSASA) needs to gather and use certain information about individuals. These can include student members, employees, or individuals within organisations who supply us with goods or services and other people the organization has a relationship with or may need to contact.

GSASA is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data. This policy describes how this personal data must be collected, handled and stored.

This policy helps to protect GSASA from data security risks, including:

- Breaches of data protection: For instance, information being given out inappropriately
- Inappropriate use of data. For example, ensuring that information provided is only used for the legitimate purposes.

This policy sits alongside GSASA's **Privacy Notice, Subject Access Request Protocol,** and **Data Retention Schedule.**

# 2. Key definitions

**Data Controller**
A data controller is the organization that decides how and why to collect and use personal data. Under GDPR, the data controller is responsible for making sure that the processing of the personal data they control complies with data protection law.

**Data processing**
Data processing includes obtaining/collecting, recording, holding, storing, organizing, adapting, analyzing, copying, transferring, combining, erasing, and destroying of information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

Data processing is carried out either by GSASA employees or members, or by organisations or individuals with whom GSASA has an agreement, for example, an online ticketing platform or cloud storage service.

**Data Protection Officer (DPO)**
The Data Protection Officer in GSASA is the **General Manager**, Lauren MacFadyen.

Whilst everyone who works for or with GSASA has some responsibility for ensuring that personal data is collected, stored and handled in accordance with this Data

Protection Policy and in line with the data protection principles, the Data Protection Officer has key areas of responsibility. The Data Protection Officer reports to the Board of Trustees about data protection responsibilities, risks and issues; reviews the organisation's data protection training, advice and policies; and deals with Subject Access Requests. The Board of Trustees is ultimately responsible for making sure that GSASA meets its legal obligations.

**Data Subject**
This is the term used for the individual whom particular personal data is about. This policy generally uses the term 'individuals' instead.

**GDPR**
The General Data Protection Regulation (EU) 2016/679.

**ICO**
The UK Information Commissioner's Office. The ICO is the supervisory authority for data protection in the UK.

**Personal data**
Personal data is information about any living individual, who is identifiable from that information or who could be identified from that information combined with other data which GSASA holds or is likely to obtain. This might be anyone, including a customer, employee, partner, member, supporter, business contact, public official or member of the public.

Personal data includes:

- Names,
- Contact information
- Student ID or 'matriculation number'
- Photographs
- Date of birth
- Bank details
- National insurance number
- Supervision notes and performance reviews
- Student complaints, including any case notes

**Sensitive personal data**
Also known as "special category" data, includes:

- Health details,
- Race and nationality
- Politics
- Trade union membership
- Religious beliefs
- Sexuality and gender identity

There are additional restrictions on the processing of sensitive personal data as, in particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. These restrictions are set out in Article 9 of the GDPR.

Personal data relating to criminal convictions and offences is categorised differently from 'special category' data, as there are further conditions on the lawful basis of processing this type of data.

## 3. Principles of data protection

GSASA is committed to processing data in accordance with its responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be collected and processed in accordance with the following 6 principles:

a. **Lawfulness, fairness and transparency**

   Personal Data must be processed lawfully, fairly and in a transparent manner. This means that GSASA must identify a lawful basis before data can be processed, as set out in Article 6 of the GDPR. GSASA must also consider whether it is fair and reasonable to process an individual's personal data, and must treat individuals fairly when they seek to exercise their rights over their data. Transparency means that GSASA must be clear, open and honest with individuals about how and why their personal data is used, using clear and plain language.

b. **Purpose limitation**

   Personal data can only be collected for specific, explicit and legitimate purposes and must not be further processed in any manner incompatible with those purposes. Further processing for archiving is permissible if certain requirements are met.

c. **Data minimization**

   Personal Data must be adequate, relevant and limited to what is necessary for processing. This includes limiting who is able to access personal data.

d. **Accuracy**

   Personal data must be adequate and, where necessary, kept up to date. If necessary, it should be erased or amended without delay.

e. **Storage limitation**

   Personal data processed for any purpose must not be kept longer than is necessary for that purpose. GSASA can store personal data for longer periods for archiving if certain requirements are met.

f. **Security and confidentiality**

Personal data must be stored in a way that ensures appropriate security including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

## 4. Data security

GSASA, its staff, members of the Board of Directors and Board of Trustees and student members, must ensure that all personal data held by them are kept securely. The responsibility for ensuring that personal data is securely protected rests with the individual handling the data.

Staff and members should speak to the Data Protection Officer and/or consult with GSA IT Department for advice if they are unsure about how to protect the security of personal data.

Unauthorised disclosure of personal data constitutes a breach of the GDPR and may also lead to disciplinary proceedings. Individuals may also face criminal proceedings for a serious breach of the provisions of the GDPR or if they knowingly or recklessly obtain and/or disclose personal data without GSASA's consent, for example, for their own purposes which are outside the legitimate purposes of GSASA.

Personal data should not be disclosed to unauthorized people, internally or externally. The only people able to access data covered by this policy should be those who need it for their work.

**Electronic data security**
Personal data should only be stored on designated drives and should only be uploaded to approved cloud computing services.

Data should be protected by strong passwords that are changed regularly and never shared.

When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

Personal data should not be saved directly onto personal devices like laptops, tablets or smart phones as there is a higher risk of these devices being lost, damaged or stolen, leading to personal data breaches (see section 6).

Personal data should not be transferred outside of the European Economic Area, unless this has been agreed by the Data Protection Officer, with an agreement with the data processor (such as a contract or terms of service agreement), and the individual knows in advance that their personal data will be treated in this way, through a privacy notice.

Personal sensitive data should be encrypted before being transferred electronically.

**Physical records of personal data**
Where personal data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it, such as in a locked filing cabinet in an office within the GSASA offices.

Employees and members processing personal data should make sure that paper and printouts are not left where unauthorized people could see them, like on a printer or on a desk.

## 5. Data retention

Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. Retention periods will be set based on legal and regulatory requirements, sector and good practice guidance. The **GSASA Data Retention Schedule** should be adhered to and is available from the Data Protection Officer.

**Data held by student members of GSASA**
Where student members process data, a retention schedule should be created and adhered to. For example, where a student society holds a membership list containing members' names and email addresses, this list should be updated at least once each academic year, and the personal data of those who are no longer members should be permanently deleted. This should be written down in a retention schedule, alongside any other membership data.

**Disposal of personal data**
Once personal data is no longer required, it should be disposed of securely.

Paper records should be shredded. Electronic records should be permanently deleted. If unsure, the IT department should be consulted on how to properly delete electronic records.

**Archiving of personal data**
GSASA deposits certain records of its business in the GSA Archives. These include the business of the Student Representative Council, including Committee minutes, election campaigns and membership records. Other aspects of GSASA are also deposited in the Archives, including students who have successfully applied for funding for extracurricular projects and the winner of the Student Life Prize.

GSASA must carefully consider the archiving of items which contain personal data and ensure that individuals are informed of this in advance, such as through the use of privacy notices.

## 6. Reporting personal data breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, unauthorized disclosure of, or access to, personal data.

GSASA must make every effort to avoid personal data breaches. However, it is possible that mistakes may occur or things might happen that are out with GSASA's control. Breaches can occur for many reasons, including loss or theft of equipment, an email sent to the incorrect recipient, hacking or 'phishing'.

As soon as a breach is discovered, it must be reported to the Data Protection Officer.

The GDPR requires that if appropriate, personal data breaches are reported to the ICO as soon as possible, and at the latest within 72 hours of GSASA becoming aware of the breach. (For more information, see ICO guidance)

Where the breach will result in a high risk to the rights and freedoms of individuals, GSASA must let those individuals know about the breach.

## 7. Individuals' rights and Subject Access Requests

The GDPR gives individuals rights about the personal data held about them:

- The right to be informed about the collection and use of their personal data
- The right of access, often known as 'subject access'
- The right to rectification if the data is incorrect or incomplete
- The right to erasure, sometimes known as 'the right to be forgotten'
- The right to restrict processing of their personal data
- The right to data portability
- The right to object to the processing of their personal data

An individual can contact GSASA, either verbally or in writing, to ask to see information that is held on them. This is called a Subject Access Request. An individual should not normally be charged for making this request.

The Data Protection Officer is responsible for processing Subject Access Requests, but all employees in the organisation should be able to recognise when a request has been made, and passing the request on to the Data Protection Officer. The **Subject Access Request Policy and Procedure** sets out how to deal with Subject Access Requests in a timely manner, and within one month.

## 8. Requests for personal data from third parties

As a rule, GSASA should never disclose personal data to an external/third party without the explicit consent of the data subject. This includes requests for references or requests from friends and family.

There are certain circumstances where GSASA is legally obliged to disclose personal data. GSASA must be satisfied that the request is legitimate, seeking assistance from the Board of Trustees and taking legal advice where necessary.

**Requests from the Home Office**
GSASA may receive requests for information about its employees. Information should only be disclosed where GSASA is satisfied that there is a legal requirement

to provide the requested information, or the individual concerned has given their consent.

**Requests from the police or law enforcement officials**
There are circumstances where GSASA is legally obliged to disclose information about an individual to a third party is this is required by statute or court order. All such requests should be submitted in writing to the Data Protection Officer.

## 9. Additional considerations

**Promoting responsible data processing practices**
GSASA should always consider whether there is a need to record personal data, and whether anonymized or pseudonymised data could be used instead.

If GSASA is setting up new systems or processes, the Data Protection Impact Assessment guideline should be followed.

**Privacy Notices**
A Privacy Notice communicates to individuals how their personal data are being used, how long they are stored for, and should let individuals know that they have rights over their personal data. Privacy Notices should be transparent and written in clear, plain language. Those within GSASA who process personal data, including members, employees and societies, need to create a Privacy Notice to accompany any point where individuals are asked to share personal data.

The Societies Handbook, available on Canvas and from the Student Engagement Team, includes example Privacy Notices for membership forms.

The Data Protection Officer can advise members and employees unsure of when to use a privacy notice, and what information should be included.

**Photography and video**
Still and moving images, where they feature identifiable individuals, are considered ‘personal data’ and must be treated with the same care. These procedures apply to still and moving images created or commissioned by GSASA employees, contractors, and members in the course of their work for GSASA.

*Individuals and small groups*
When taking photographs or filming an individual or a small group, it’s most appropriate to get each individual’s consent with a simple form. It should be clearly communicated to the images will be used for - for example, for societies, it’s likely that such images will be shown to the SRC and the Students’ Association, and used on societies’ social media to promote the society and document its activities.

*Crowds and large events*
Notices should be placed prominently, such as at the entrance to the venue and at clear points within the venue, to alert individuals to filming and photography taking place. When someone enters the event venue, signs in or gives a ticket would be a good time to tell them about photography/filming that is happening. Wherever possible, it should be clear and easy for a person to opt-out of having their picture taken.

*When to consider using an opt-in approach to consent at larger events*
Where events are about more sensitive topics, or have people with shared experience of oppression as intended participants and focus, it may be more appropriate to consider using an opt-in approach (instead of assuming that everyone is happy to be photographed unless they tell you otherwise).

*CCTV*
CCTV cameras are located both on the outside and within the Art School building, in compliance with licensing regulations. Notices should be placed around the building, advising people of the presence of these cameras.

**Direct marketing**
Direct marketing is defined in the Data Protection Act 2018 as “the communication (by whatever means) of advertising or marketing material which is directed to particular individuals”. Direct marketing includes messages promoting an organisation’s values or beliefs, services or events. This includes mailing lists.

Consent is required for direct marketing messages. This means that individuals must ‘opt-in’ to receiving messages and must be able to withdraw their consent at any point. For mailing lists, this might look like having an unsubscribe link at the top or bottom of every email communication. In addition, the GDPR requires that evidence of consent is kept.

Not all email communications are treated in this way, even if you are emailing many individuals at once. Service messages do not have to be treated in this way, as there will likely already be another lawful basis under which personal data is processed. If the answer to any of the following questions is “yes”, it is likely to be a service message and not a ‘direct marketing’ message.

- Is GSASA under a legal obligation to send this message?
- Is the message part of carrying out a contract?
- Would the individual be at a disadvantage if they did not receive the message?

**Data Protection Impact Assessment**
A Data Protection Impact Assessment (DPIA) is a process to help identify and minimize the data protection risks of a project, before any personal data processing has taken place.

Whilst it is good practice to do a DPIA before starting any major project which requires processing personal data, a DPIA *must* be done for any data processing that is likely to result in a high risk to individuals.

The ICO provides guidelines and further information on when a DPIA must be carried out. The ICO should be consulted if, after creating a DPIA, a high risk is identified that cannot be mitigated. (See ICO guidance.)

A DPIA template is available from the DPO.

## 10. Further resources

*ICO Guide to the GDPR*
The website of the Information Commisioner's Office provides comprehensive guidance on Data Protection and the GDPR.

> https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

*Lawful Basis Guidance Tool for organisations*
Assistance in establishing what lawful basis your data processing may fall under. This tool is a useful step in establishing whether it is lawful to process a type of personal data, as part of a Data Protection Impact Assessment

> https://ico.org.uk/for-organisations/resources-and-support/lawful-basis-interactive-guidance-tool/